ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Symbolic Computation 41 (2006) 297–316

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Tree polynomials and non-associative Gröbner bases

Lothar Gerritzen*

Ruhr-Universität Bochum, Fakultät für Mathematik, Gebaude Na 2/33, D 44780 Bochum, Germany

Received 14 February 2003; accepted 8 September 2003
Available online 6 October 2005

Abstract

In this article the basic notions of a theory of Gröbner bases for ideals in the non-associative, non-commutative algebra $K\{X\}$ with a unit freely generated by a set X over a field K are discussed. The monomials in this algebra can be identified with the set of isomorphism classes of X-labelled finite, planar binary rooted trees where X is the set of free algebra generators. The elements of $K\{X\}$ are called tree polynomials. We describe a criterion for a system of polynomials to constitute a Gröbner basis. It can be seen as a non-associative version of the Buchberger criterion.

A formula is obtained for the generating series of a reduced Gröbner basis for the ideal of non-associative and non-commutative relations of an algebra relative to a system of algebra generators and an admissible order on the monomials. If the algebra is graded it specializes to a general Hilbert series formula in terms of generators and relations.

We also report on new results concerning non-associative power series like exp, log and the Hausdorff series $\log(e^x e^y)$ and on problems related to Hopf algebras of trees. Reduced Gröbner bases for closed ideals in tree power series algebras $K\{\{X\}\}$ are considered.

Keywords: Free magmas; Planar binary rooted trees; Non-associative free algebras; Ideals; Gröbner bases; Non-associative Buchberger criterion; Composition lemma; Diamond lemma; Hilbert series; Tree power series; Non-associative exponential and logarithm; Cayley numbers; Free alternative algebra

1. Introduction

In the first volume on algebra of the Encyclopedia of Mathematical Sciences published by the Academy of Sciences of the USSR in 1987, the author I.R. Shafarevich also presents his general

* Tel.: +49 234 32 28304; fax: +49 234 32 14025.
E-mail address: lothar.gerritzen@ruhr-uni-bochum.de.

doi:10.1016/j.jsc.2003.09.005

views about basic notions of algebra. He has attempted a description of the place in mathematics occupied by algebra by drawing attention to the process of measuring for which H. Weyl has coined the word coordinatization. This general idea is certainly of great importance because it challenges the Bourbaki view that algebra is a certain theory of structures of composition laws. However, since the appearance of computer algebra this recent approach to describing algebra generally also seems to be insufficient.

Later in this treatise, Lie algebras, Cayley numbers and other types of non-associative algebra are discussed. It is stated that no general theory of non-associative algebras exists at present and the question is raised of whether such a theory is perhaps just not possible (Shafarevich, 1990), Section 19, D. (p. 201).

It seems to me that this scepticism derived from the principle of coordinatization is no longer justified.

The non-associative, non-commutative algebra freely generated by one element x has a vector space basis given by the set of finite planar, binary rooted trees and it is nowadays completely clear that these objects are indispensable in computer science and other theoretical branches for abstract measurings, searchings and designs; see Knuth (1973).

In this context one should also mention the many publications on Hopf algebras of trees—see Connes and Kreimer (2000), Loday and Ronco (1998) and Brouder and Frabetti (2003)—and recent work on operads—see Ginzburg and Kapranov (1994)—or the non-associative exponential, logarithm and Hausdorff series (Drensky and Gerritzen, 2002; Gerritzen and Holtkamp, 1998).

In this note an interesting algorithmic and computational theory of Gröbner bases for ideals in the non-associative noncommutative K-algebra $K\{X\}$ with a unit element freely generated by a set X of variables over a field K is considered. It can be seen as a branch of a general theory of non-associative or tree algebra.

A K-vector space basis for $K\{X\}$ is the magma $Mag'(X)$ with a unit freely generated by X; see Bourbaki (1971). There are admissible orders $<$ on $Mag'(X)$ and for a non-zero polynomial f in $K\{X\}$ one has the leading term $f^{<}$ in $Mag'(X)$ of f.

A system Γ of generators for an ideal I in $K\{X\}$ is a Gröbner basis if the leading term $f^{<}$ of any non-zero f in I is a multiple of an element $g^{<}, g \in \Gamma$, in $Mag'(X)$; see Section 5.

There is a criterion which guarantees that a given set of polynomials is a Gröbner basis. It appears as a non-associative version of the criterion of Buchberger; see Section 6. It can also be seen as a general form of the Diamond Lemma of Bergman—see Bergman (1978)—or the Composition Lemma—see Ufnarovskij (1995), Chap. I, Section 2.5, p. 30.

There are procedures similar to the Buchberger algorithm (Buchberger, 1965) for constructing non-associative Gröbner bases; see Section 7.

In Section 2 we introduce the magma $PB(X)$ of finite, X-labelled planar binary rooted trees where the composition law is provided by grafting. It is shown that $PB(X)$ is canonically isomorphic with the free magma $Mag(X)$. If T is a tree in $PB := PB(\{x\})$ with n leaves and $v_1, \ldots, v_n$ is a sequence of elements in any magma N, one can substitute it into T and obtain a well-defined element $T(v_1, \ldots, v_n)$ in N, as T can be interpreted as a well-suited system of bracketing. If $v_1, \ldots, v_n$ are in $PB(X)$, then $T(v_1, \ldots, v_n)$ is the tree which is obtained from T by identifying the root of v_i with the ith leaf of T. This operation is inverse to the construction of admissible cuttings in the theory of Hopf algebras of trees; see Connes and Kreimer (2000).

Admissible orders on $Mag'(X)$ are considered in Section 3 and a special class of orders which are called degree first factor orders is introduced. It is an open problem to determine all admissible orders on $Mag'(X)$.

Ideals in free magmas are the topic in Section 4. Any such ideal has a unique minimal set of generators. It is easy to see that $w \in PB(X)$ is a multiple of $v \in PB(X)$ if and only if there is a node q in w such that the subtree below q in the direction of the leaves of w is isomorphic with v. We prove a simple, but basic lemma which states that if $w_1, \ldots, w_n \in PB(X)$ and if w_j is not contained in the principal ideal $\langle w_i \rangle$ generated by w_i for $j \neq i$, then an element v in the intersection $\langle w_1 \rangle \cap \cdots \cap \langle w_u \rangle$ can be written as $T(u_1, \ldots, u_r)$ and for all i there is an element j such that $u_j = w_i$.

From this we can derive that there are no problems with overlaps corresponding to s-polynomials in the theory of non-associative Gröbner bases. This is in contrast to the associative case; see Bergman (1978) and Ufnarovskij (1995), Chap. I (2.3).

In Section 8 we give a general formula for the Hilbert series of any graded algebra in terms of the generating series $G_X(t)$ of a homogeneous system X of generators and the generating series $G_\Gamma(t)$ of the reduced Gröbner basis Γ of the ideal of all relations of A, considered as a homogeneous ideal in $K\{X\}$.

The result of Section 8 can be generalized to non-graded algebras. This is achieved in Section 9.

The theory of Gröbner bases can also be developed for the general algebra of power series. We give some indications in Section 10. We also give the definition of the non-associative exponential $\exp(x)$. It is the unique series $E(x)$ such that $E(x) \cdot E(x) = E(2x)$ and $E(x) = 1 + x +$ higher terms. The non-associative logarithm $\log(1 + x)$ is also defined by a functional equation and the Hausdorff series is introduced. Some groups of automorphisms of tree power series algebra have a dual which is a Hopf algebra. There is an interesting relation with the Hopf algebra of Connes and Kreimer; see Connes and Kreimer (2000) and Foissy (2002).

Finally we consider two examples. The infinite Gröbner basis for the free associative algebra is derived in Section 11. It is an open problem to find the reduced Gröbner basis for the free alternative algebras. This is described in Section 12.

2. On free magmas and trees

A magma is a set N together with a binary operation on N which will usually be denoted by $\cdot_N$ or a dot.

This notion was introduced by Bourbaki (1971), Chap. 1, Section 1. It has initialized the name of the algebraic programming language Magma; see Cannon and Playoust (1997), Section (4.1), p. 46.

Let X be a non-empty set.

Proposition 2.1. *There is a magma $Mag(X)$ with the following properties:*

(i) *X is a subset of $Mag(X)$.*

(ii) *The multiplication on $Mag(X)$ is an injective map $\cdot : Mag(X) \times Mag(X) \to Mag(X)$ and the image of $\cdot$ is the complement of X in $Mag(X)$.*

$Mag(X)$ is uniquely determined by X up to isomorphisms and is called the magma freely generated by X. It corresponds to the absolutely free algebra generated by X with respect to a single binary operation.

Proof. The construction of $Mag(X)$ can be found in the literature; see for instance Bourbaki (1971) and Gerritzen (1994). □

There is a unique morphism $deg : Mag(X) \to \mathbb{N}$, such that $deg(x) = 1$ for all $x \in X$ where $\mathbb{N}$ denotes the additive monoid of natural numbers. Then $deg(v)$ is called the degree of $v \in Mag(X)$.

Let T be a finite rooted tree; see Harary (1968), Chap. 15, p. 187. We denote by T^0 the set of nodes (vertices) of T, by $\bar{T}$ the set of edges of T and by w_T the root of T.

For any node a of T we denote by $val_T(a)$ the valence of T. It is the number of edges of T which are incident with a.

Definition. T is called binary if $val_T(w_T) \in \{0, 2\}$ and $val_T(a) \in \{1, 3\}$ for any node $a \neq w_T$ of T.

The nodes a of T with $val_T(a) \leq 1$ are called leaves (or end nodes) of T. $L(T)$ denotes the set of leaves of T. If there is a node a in T with $val_T(a) = 0$, then T consists of a single node.

Definition. A finite binary tree T together with a dissection $\bar{T} = \bar{T}^1 \dot{\cup} \bar{T}^2$ of the set of edges of T is called planar if for any node a of T which is not a leaf of T there are edges $k_1 \in \bar{T}^{(1)}, k_2 \in \bar{T}^{(2)}$ incident with a and if $a \neq w_T$ then neither lies on the unique simple path from the rooted w_T to a. The edges in $\bar{T}^{(1)}$ (resp. $\bar{T}^{(2)}$) are called the left (resp. right) edges of T.

Definition. A finite planar binary rooted free T together with a map

$$\lambda : L(T) \to X$$

is called X-labelled.

Let T_1, T_2 be two finite planar binary rooted trees and let φ be a bijective map $T_1^0 \to T_2^0$. Then φ is called an isomorphism from T_1 onto T_2 if φ maps the root of T_1 onto the root of T_2 and if the map induced by φ on the system $Pot(T_1^0)$ of the subsets of T_1^0 maps $\bar{T}_1^{(i)}$ onto $\bar{T}_2^{(i)}$ for $i = 1, 2$. Then $\varphi(L(T_1)) = L(T_2)$. If λ_i is an X-labelling of T_i, then φ is an isomorphism from (T_i, λ_1) into (T_2, λ_2) if φ is an isomorphism of planar binary rooted trees and $(\lambda_2 \circ \varphi)|L(T_1) = \lambda_1$.

Let $PB(X)$ denote the set of all isomorphism classes of X-labelled finite planar binary rooted trees.

If $T, T' \in PB(X)$, then there is a unique $T \cdot T' \in PB(X)$ with the following properties: if the root of $T \cdot T'$ and the edges incident with it are removed from $T \cdot T'$, then the components of connectivity of this remaining graph consist of T and T'. This operation is called grafting and turns $PB(X)$ into a magma.

If $X = \{x\}$, then all labels of all elements in $PB(\{x\})$ are x and we can forget them. $PB(\{x\})$ is then called the magma of finite planar binary rooted trees and is also denoted by PB.

The following fact is fundamental for free magmas because it shows that there is an canonical combinatorial structure on the elements of $Mag(X)$. Strangely this view was not included in the presentations of free magmas by Bourbaki (1971), or in the discussion by Kurosh (1947), of general free algebras. Maybe this was one reason that the general theory of non-associative algebras did not flourish for some decades in the last century.

The proof of the following statement is simple; see also Reutenauer (1993), p. 5 or Gerritzen (2000).

Proposition 2.2. (i) *There is a unique morphism*

$$\eta : Mag(X) \to PB(X)$$

such that $\eta(x)$ is a tree consisting of a node only labelled with x whenever $x \in X$.

(ii) *η is an isomorphism of magmas.*

(iii) *For any* $v \in Mag(X)$, $deg(v)$ *is equal to the number of leaves of* $\eta(v)$.

Proof. (1) Let $v \in Mag(X)$, $n = deg(v)$. We define $\eta(v)$ by induction on n. If $n = 1$, then $v \in X$ and $\eta(v)$ is already defined. If $n > 1$, then $v = v_1 \cdot v_2$, $v_i \in Mag(X)$ and $deg(v_i) < n$. By the induction hypothesis $\eta(v_i)$ is already defined and $\eta(v) := \eta(v_1) \cdot (v_2)$. Obviously η is a morphism, because there is only one decomposition of v into two factors.

(2) Let $T \in PB(X)$ and let $l(T)$ denote the number of leaves of T. We want to show that η is surjective by induction on $l(T)$.

If $l(T) = 1$, then T has only one node and $T = \eta(x)$ for some $x \in X$. If $l(T) > 1$, then $T = T_1 \cdot T_2$ with $T_i \in PB(X)$ and $L(T) = L(T_1)\dot{\cup}L(T_2)$ and thus $l(T) = l(T_1) + l(T_2)$.

By the induction hypothesis there are $v_i \in Mag(X)$ such that $\eta(v_i) = T_i$. Then $\eta(v) = T$ if $v = v_1 \cdot v_2$.

(3) Using the argument in (2) one can also show that $deg(v) = l(\eta(v))$ for all v. This proves statement (iii).

(4) Assume that η is not injective. Then there are $v, w \in Mag(X)$, $v \neq w$, such that $\eta(v) = \eta(w)$.

We choose the pair v, w such that $n = deg(w)$ is minimal. Then $n = deg(v)$ by (3) and $n > 1$, because for $n = 1$ the tree $\eta(v)$ has only one node.

Let $v = v_1 \cdot v_2$, $w = w_1 \cdot w_2$ be decompositions in $Mag(X)$ and $\eta(v_i) = T_i$, $\eta(w_i) = S_i$. Then $T_1 \cdot T_2$ is isomorphic to $S_1 \cdot S_2$. An isomorphism from $T_1 \cdot T_2$ onto $S_1 \cdot S_2$ maps the root of $T_1 \cdot T_2$ to the root of $S_1 \cdot S_2$ and obviously also the subtree T_i of T to S_i. Thus it induces isomorphisms $T_i \to S_i$. It follows that $v_i = w_i$, as $deg(v_i) < n$. This is a contradiction to the assumption $v \neq w$. □

Let PB be the magma of finite planar binary rooted trees.

Let $T \in PB$ and $l(T) =: deg(T) = n$. The set $L(T)$ of leaves of T is a canonically ordered set. This ordering is defined by induction on n. This is trivial for $n = 1$. If $n > 1$ and $T = T_1 \cdot T_2$ we may assume that the set $L(T_i)$ of leaves of T_i is already ordered. This leads to an order on $L(T) = L(T_1)\dot{\cup}L(T_2)$ on defining $b_1 < b_2$ for any $b_1 \in L(T_1)$, $b_2 \in L(T_2)$.

Now let N be any magma and $v_1, \ldots, v_n \in N$.

We want to define $T(v_1, \ldots, v_n)$ by induction on n.

If $n = 1$, then it is v_1. If $n > 1$ and $T = T_1 \cdot T_2$, then

$$T(v_1, \ldots, v_n) = T_1(v_1, \ldots, v_{n_1}) \cdot T_2(v_{n_1+1}, \ldots, v_n)$$

if $n_1 = deg(T_1)$.

Informally $T(v_1, \ldots, v_n)$ is the product of $v_1, \ldots, v_n$ according to the bracketing induced by the tree $T \in PB$.

3. Admissible orderings on free magmas

A well-ordering $<$ on the free magma $M = Mag(X)$ is called admissible if:

(i) Whenever $a, b, c \in M$ and $a < b$, then $ac < bc$ and $ca < cb$.
(ii) Whenever $a, b \in M$, then $a < ab$ and $a < ba$.

We give the construction of an admissible ordering $<_{deg,1}$ on M which will be called the degree first factor ordering.

Fix a well-ordering on X.

Let $v, w \in M$, $v \neq w$.

Define $v <_{deg,1} w$ if $deg(v) < deg(w)$.
Assume now that $deg(v) = deg(w) = k$.
Define $v <_{deg,1} w$ if $v, w \in X$ and v is smaller than w relative to the fixed ordering on X.
Assume now that $v, w \notin X$. Then $k > 1$ and $v = v_1 v_2$, $w = w_1 w_2$ with $v_i, w_i \in M$ and $deg(v_i) < k$, $deg(w_i) < k$ for all i.
By induction on k we define $v <_{deg,1} w$ if $v_1 <_{deg,1} w_1$ or $v_1 = w_1$ and $v_2 <_{deg,1} w_2$. Then $<_{deg,1}$ is a well-ordering because one can prove by induction on n that any subset of $\{v \in Mag(X) : deg(v) = n\}$ has a minimal element.
Assume that D is a subset of $Mag(X)$ of elements of degree n. We prove by induction on n that D has a minimal element relative to $<_{deg,1}$. If $n = 1$, it has a minimal element, because $D \subseteq X$. If $n > 1$ and k is the minimal degree of the first factors of the elements in D, then $k < n$. Also the set D_k of all the first factors of elements from D of degree k has a minimal element v. Let $\bar{D}$ be the set of second factors of elements from D whose first factor is v. By the induction hypothesis $\bar{D}$ has a minimal element w. Then $v \cdot w$ is minimal in D.

In a similar way one can define a degree second factor order $<_{deg,2}$ on $Mag(X)$.

Let $Mag'(X)$ be obtained from $Mag(X)$ by adjoining a neutral element which will be denoted by 1_X or 1. It will be called a magma with a unit freely generated by X. Any admissible order $<$ on $Mag(X)$ can be extended to $Mag'(X)$ by defining $1 < v$ for any $v \in Mag(X)$.

4. Ideals in free magmas

Let N be a magma, $a, b \in N$.

Definition. b is called a multiple of a in N if there is a sequence

$$p = (c_0, \ldots, c_r), r \geq 0$$

such that $c_0 = a$, $c_r = b$, and $c_{i+1} = c_i \cdot d_i$ or $c_{i+1} = d_i \cdot c_i$ for all $0 \leq i < r$ with $d_i \in M$.

We also call p a path from a to b in N.

If b is a multiple of a in N, we also call a a divisor of b in N.

Let $I \subset N$, $I \neq \emptyset$.

Definition. I is called an ideal in N if for all $a \in I$, $b \in N$, the elements $a \cdot b, b \cdot a \in I$.

It is easy to see that the set $< a >_N$ of all multiples of $a \in N$ in N is an ideal in N. It is the smallest ideal containing a and is also called the principal ideal generated by a.

The multiples of $v \in Mag'(X)$ in $Mag'(X)$ are the multiples of v in $Mag(X)$ if $v \neq 1$. If $v = 1$ then all elements in $Mag'(X)$ are multiples of v.

Proposition 4.1. *Let I be an ideal in $Mag'(X)$. There is a unique minimal set $\Omega \subset I$ such that*

$$I = \bigcup_{v \in \Omega} < v >_{Mag'(X)}$$

where Ω is called the ideal basis of I.

Proof. If the neutral element 1_X of $Mag'(X)$ is contained in I, then $I = < 1_X >$.

Assume now that $1_X \notin I$.

Let

$$\Omega := I - (I \cdot Mag(X) \cup Mag(X) \cdot I)$$

where Ω is the union of $I \cap X$ with the set of all

$$\omega = v \cdot w \in I$$

with $v, w \in Mag(X)$ and $v \notin I$ or $w \notin I$. I claim that

$$I = \cup_{\omega \in \Omega} < \omega >$$

Obviously $< \omega > \subset I$ for all $\omega \in \Omega \subseteq I$.
Now let $t \in I, deg(t) = n$.
We show by induction on n that $t \in < \omega >$ for some $\omega \in \Omega$.
If $n = 1$, then $t \in \Omega$. Consider now $n > 1$. If $t \notin \Omega$, there is a decomposition

$$t = v \cdot w$$

with $v, w \in Mag(X)$ and $v \in I$ or $w \in I$.

Thus $v \in < \omega >$ or $w \in < \omega >$ as $deg(v) < n$, $deg(w) < n$ by the induction hypothesis. But then clearly $t \in < \omega >$. □

There is the following combinatorial description of the principal ideals in $Mag'(X)$.

Let $v \in Mag'(X)$ and $T = \eta(v)$ be the tree in $PB(X)$ according to Proposition 2.2.

Let a be a node of T and T_a the subtree of T whose nodes consist of all nodes b of T for which the simple path from the root of T to b passes through a.

If a is designed as a root of T_a then T_a has a canonical structure of a planar binary rooted tree and v_a is the unique element in $Mag(X)$ such that $\eta(v_a) = T_a$.

Proposition 4.2. *The principal ideal in $Mag'(X)$ generated by an element $t \in Mag(X)$ consists of all $v \in Mag(X)$ for which there is a node a such that $v_a = t$.*

Proof. (1) Let a be a node of $S_1 \cdot S_2$, $S_i \in PB(X)$. Then a is a node of S_1 or of S_2 or it is the root of $S_1 \cdot S_2$. If it is a node of S_i, then $(S_1 \cdot S_2)_{\leq a} = (S_i)_{\leq a}$. If it is the root of $S_1 \cdot S_2$, then $(S_1 \cdot S_2)_{\leq a} = S_1 \cdot S_2$.

(2) From (1) it follows easily that all the multiples S of $T \in PB(X)$ in $PB(X)$ have a node a with $S_{\leq a} = T$.

(3) Let $T, S \in PB(X)$ and assume that there is a node a in S such that $S_{\leq a} = T$. We prove that S is a multiple of T by induction on $l(S)$. If a is the root of S, then $S_{\leq a} = S$ and $T = S$.

If a is not the root of S, then $S = S_1 \cdot S_2$ and a is a root of S_i for $i = 1$ or $i = 2$. Then $S_{\leq a} = (S_i)_{\leq a}$. As $l(S_i) < l(S)$ we may assume that S_i is a multiple of T. Then S is also a multiple of T. □

Example. Let $\Omega := \{x^n \cdot x^m : n, m \geq 2\} \subseteq Mag(\{x\})$. Then the magma ideal I generated by Ω in $Mag(\{x\})$ has Ω as a basis, because if a is a node in the tree $\eta(x^n \cdot n^m) = T$, but not the root of T, then $T_{\leq a} = \eta(x^k)$ for some k. It follows that $x^n \cdot x^m$ is not a multiple of $x^{n'} \cdot x^{m'}$ if $(n', m') \neq (n, m)$. By Proposition 4.1 it follows that I has no finite set of generators.

The following result is used in the proof of Proposition 4.3.

Lemma 4.1. *Let q_1, q_2 be nodes of $T \in B$ and assume that the subtrees $T_1 = T_{\leq q_1}, T_2 = T_{\leq q_2}$ of T have a common node.*

Then T_1, T_2 can also be considered as elements of PB and then T_1 is a divisor or a multiple of T_2 in PB.

Proof. Let v be a node in T which belongs to T_1 and T_2. Let P be the simple path in T from the root of T to v. It passes through q_1 and q_2. If it first passes through q_1, then $T_2 \subseteq T_1$ and T_2 is a divisor of T_1 in B. Otherwise $T_1 \subseteq T_2$ and T_1 is a divisor of T_2 in PB. $\square$

Proposition 4.3. *Let $w_1, \ldots, w_n \in Mag(X)$ and assume that w_i is not a multiple of w_j for all $i \neq j$.*

Let $< w_i >$ be the principal ideal in $Mag(X)$ generated by w_i and

$$I = < w_1 > \cap \cdots \cap < w_k > .$$

Then I is an ideal in $Mag(X)$ and $v \in Mag(X)$ is in I if and only if there is a tree $T \in PB$ and $u_1, \ldots, u_n \in X \cup \{w_1, \ldots, w_k\}$ of degree n such that

$$v = T(u_1, \ldots, u_n)$$

and such that for all i there is a j with $u_j = w_i$.

Proof. (1) If $v = T(u_1, \ldots, u_n)$ with the properties in the statement above, then $v \in < w_i >$ for all i by Proposition 4.1. Thus $v \in I$.

(2) Let $v \in I$ and Q be the set of nodes q of the tree $S = \eta(v) \in PB(X)$ for which the subtree $S_{\leq q_1}$ is contained in $\{\eta(w_1), \ldots, \eta(w_k)\}$. Then $S_{\leq q'} \cap S_{\leq q} =$ empty for $q \neq q'$; see Lemma 4.1.

If we remove all non-root nodes of $S_{\leq q}$ for all q, we get a tree $T \in PB$.

If the i-th leaf of T is a leaf of S, then we put $v_i =$ a label of S at this leaf. If $q \in N$, then $v_i := w_j$ if $\eta(w_j) = S_{\leq q}$.

Then $T(v_1, \ldots, v_n) = S$ and for any i there is j such that $w_i = v_j$. $\square$

5. Gröbner bases of ideals in free algebras

Denote by $K\{X\}$ the magma algebra of $Mag'(X)$ over a field K. This object was studied by Kurosh in Kurosh (1947) and also occurs in the work of Lazard; see Lazard (1955). A K-vector space base of $K\{X\}$ is $Mag'(X)$.

Let I be a K-subvector space of $K\{X\}$.

Definition. I is called an ideal of $K\{X\}$ if $f \cdot g, g \cdot f \in I$ whenever $f \in I$ and $g \in K\{X\}$.

Let $F \subset K\{X\}$. There is a smallest ideal $I(F)$ in $K\{X\}$ which contains F.

Let $f, g \in K\{X\}$.

Definition. g is called a multiple of f in $K\{X\}$ if there is a sequence $p = (f_0, f_1, \ldots, f_r), r \geq 0$, such that:

(i) $f_0 = f,\ f_r = g,\ f_i \in K\{X\}$.
(ii) $f_i = h_i \cdot f_{i-1}$ or $f_i = f_{i-1} \cdot h_i$ with $h_i \in K\{X\}$.

Proposition 5.1. *$I(F) =$ the K-vector space generated by $\bigcup_{f \in F} \langle f \rangle$ where $< f >$ denotes the set of all multiples of f in $K\{X\}$.*

Let $<$ be an admissible order on $Mag(X)$ and $f \in K\{X\},\ f \neq 0$.

We denote the leading term of f relative to this order by $f^<$ and consider $f^<$ as element in $Mag(X)$. The leading coefficient of f is denoted by $c(f) \in K$.

Then the leading term of $f - c(f) \cdot f^<$ is less than $f^<$.

Now let I be an ideal in $K\{X\}$, $I \neq \{0\}$ and $F \subset I, 0 \notin F$. Then $I^< := \{f^< : f \in I, f \neq 0\}$ is a magma ideal in $Mag(X)$.

At this point we do not assume F to be finite, because ideals in $K\{X\}$ are not always finitely generated even if $\sharp X = 1$; see Proposition 11.1 or the Example after Proposition 4.2.

Definition. F is called a Gröbner basis of I if the ideal $I^<$ is generated by $F^< := \{f^< : f \in F\}$.

Remark. Comments on the history on the theory of Gröbner bases have been collected by Ufnarovskij in Ufnarovskij (1995), Chap. I, (2.12), p. 42. There is some justification for calling them Gröbner–Shirshov bases instead. A recent book on associative, non-commutative Gröbner bases was published by H. Li; see Li (2002). Gröbner bases in non-associative free algebras were already published in de Graaf and Wisliceny (1999) and Gerritzen (2000).

Assume now for simplicity that $c(f) = 1$ for all $f \in F$.
Now we introduce a relation $\mapsto_F$ on $K\{X\}$ which will be called the relation of elementary reductions relative to F.
Let $h \in K\{X\}$, $h \neq 0$, and let w be a term in h whose coefficient $c_w(f) \neq 0$. Assume that $f \in F$ and that the leading term $f^<$ of f is a factor of w in $Mag(X)$.
Let $p = (v_0, v_1, \ldots, v_r)$ be the path from $v_0 = v$ to $v_r = f^<$.
We construct a sequence $(f_0, \ldots, f_r)$ as follows: $f_0 := f$ and if f_{i-1} is already defined and if $v_i = v_{i-1} \cdot u_i$ with $u_i \in Mag(X)$, then $f_i := f_{i-1} \cdot u_i$.
If however $v_i = u_i \cdot v_{i-1}$ with $u_i \in Mag(X)$, then $f_i := u_i \cdot f_{i-1}$.
Then w is the leading term of f_r and the coefficient of f_r relative to the term w is equal to 1.
Let $h' := h - c_w(h) \cdot f_r$. Then the coefficient of h' relative to the term w is zero. Define $h \mapsto_F h'$ if h' is obtained from h in the procedure constructed above.

Let $\mapsto_F^*$ be the reflexive and transitive closure of $\mapsto_F$ and $N(F)$ be the space of all $h \in K\{X\}$ for which no term of h with coefficient $\neq 0$ is a multiple of any $f^<$, $f \in F$.

$N(F)$ is a vector space. Its elements are called normal polynomials with respect to F.

Proposition 5.2. *For any $h \in K\{X\}$, $h \neq 0$, there is $h' \in N(F)$ such that $h \mapsto_F^* h'$.*

We call h' a normal form of h with respect to F. It is not uniquely defined by h in general.

The importance of Gröbner bases can be seen in the following result, which can be called the Macauley decomposition. Its proof is completely analogous to the commutative and non-commutative cases; see Becker and Weispfennig (1993); Mora (1994); Madlener and Reinert (1993).

Corollary 5.1. (i) *$N(F) \oplus I(F) = K\{X\}$ if F is a Gröbner basis of $I(F)$.*

(ii) *The restriction of the residue class homomorphism $K\{X\} \to K\{X\}/I(F)$ onto $N(F)$ is bijective.*

Definition. A Gröbner basis G of an ideal I in $K\{X\}$ is called reduced if:

(i) all polynomials $g \in G$ are unitary;
(ii) $g_1^< \neq g_2^<$ for $g_1, g_2 \in G$, $g_1 \neq g_2$;
(iii) $\{g^< : g \in G\}$ is the basis of the magma ideal $I^<$;
(iv) if t is a term occurring in $g - g^<$, then $t \notin I^<$.

Remark. The theory of Gröbner bases should also be presented in free algebras over rings, for example over Zacharias rings. This can be done by using methods from Zacharias (1978).

6. Gröbner basis criterion

Let $F \subseteq K\{X\}$ and assume that all $f \in F$ are unitary, i.e. $c(f) = 1$.
Let $f, g \in F$, $f \neq g$.

We want to define the s-polynomial $spol(f, g)$ of f and g.

Case 1: $f^<$ is a factor of $g^<$.

Let $p = (v_0, \ldots, v_r)$ be the path between $f^<$ and $g^<$.

Then a sequence $(s_0, \ldots, s_r)$ is defined by putting $s_0 = f$. If s_{i-1} is already defined, then

$$s_i = u_i s_{i-1} \qquad \text{if } v_i = u_i v_{i-1}$$
$$s_i = s_{i-1} u_i \qquad \text{if } v_i = v_{i-1} u_i$$

Then

$$spol(f, g) := s_r - g$$

Case 2: $g^<$ is a factor of $f^<$.

Then $spol(f, g) := -spol(g, f)$.

Case 3: $g^<$ is not a factor and not a multiple of $f^<$. Then $spol(f, g) := 0$.

The following statement is the generalization of the classical criterion of Buchberger.

It is simple because there are no overlaps as in the non-commutative case.

Proposition 6.1. *F is a Gröbner basis of $I = I(F)$ if $spol(f, g) \mapsto^*_F 0$ for all $f, g \in F$, $f \neq g$.*

Proof. (1) Let $f_1, \ldots, f_r \in K\{X\}$, $v_i = f_i^< \in Mag(X)$ and assume that no v_i is a proper multiple of v_j in $Mag(X)$ for all i and j. Let $h = h_1 + \cdots + h_r$, $h_i \in < f_i > :=$ the ideal in $K\{X\}$ generated by f_i and $h_i \neq 0$ for all i.

Let $m := max_{i=1}^r(h_i^<)$. We may assume that $h_i^< = m$ for $1 \leq i \leq r'$ and $h_i^< < m$ for $r' < i \leq r$. Then $r' \geq 2$.

From Proposition 4.3 we get a finite, planar binary rooted tree $T \in PB$ of degree n and $u_1, \ldots, u_n \in \{v_1, \ldots, v_r\} \cup (X)$ such that

$$m = T(u_1, \ldots, u_n)$$

and for each $i \leq r'$ there is an index j such that $u_j = v_i$.

Now let $\tilde{u}_i := f_j$ if $u_i = v_j$ and let $\tilde{u}_i = u_i$ if $u_i \notin \{v_1, \ldots, v_r\}$. Then $\tilde{m} := T(\tilde{u}_1, \ldots, \tilde{u}_n) \in K\{X\}$ and $\tilde{m} \in < f_i >$ for $i \leq r'$.

For any i, $1 \leq i \leq r'$, there is a $\lambda_i \in K$ such that $c(h_i) = \lambda_i$. We put $\lambda_i = 0$ for $i > r'$ and let $\tilde{h}_i := h_i - \lambda_i \tilde{m}$.

Then $\tilde{h}_i \in < f_i >$ for all i because one can check that $h_i^< \in < v_i >$ for $1 \leq i \leq r'$.

Assume now that $h^< < m$. Then $\sum_{i=1}^{r'} \lambda_i = 0$ and $\sum_{i=1}^{r} \tilde{h}_i = h$.

It is easy to check that $\tilde{h}_i^< < m$ for all i.

By using this construction several times we obtain a decomposition

$$h = h'_1 + \cdots + h'_r$$

with $h'_i \in < f_i >$ and $(h'_i)^< = h^<$ for some i, $(h'_j)^< \leq h^<$ for all j.

(2) Let $G := \{g \in F$: no proper factor of g in $Mag(X)$ is contained in $F^<\}$. Using the construction in (1) one can prove that G is a Gröbner basis of the ideal $I(G)$ generated by G. By induction on $deg(f)$ and the fact that f can be reduced relative to G to zero one can show that $F \subseteq I(G)$.

Thus F is a Gröbner basis of $I(F) = I(G)$. $\square$

The following result is also contained in Bokut and Kukin (1994), Appendix 3.

Corollary 6.1. *Let* $f_1, \ldots, f_r \in K\{X\}$, $f_i \neq 0$, $f_i \in Mag(X)$ *and assume that* $f_i^<$ *is not a divisor of* $f_j^<$ *for* $i \neq j$ *in* $Mag(X)$. *Then* $\{f_1, \ldots, f_r\}$ *is a Gröbner basis of the ideal in* $K\{X\}$ *generated by* $f_1, \ldots, f_r$.

Remark. It seems to be of interest to extend the notion of Gröbner bases to more general objects in universal algebra; see Burris and Sankappanavar (1981), Chap. II, §1, §10.

A case of particular importance seems to be the algebra whose system of monomials is the set P of all planar rooted trees, which are not necessarily binary. The grafting defines n-ary operations $P^n \to P$ for all $n \geq 1$.

7. Algorithm for constructing Gröbner bases

Let $F = \{f_1, \ldots, f_n\}$ be a system of polynomials in $K\{X\}$, $f_i \neq 0$, and $I = I(F)$ the ideal generated by F.

We want to sketch a simple algorithm for computing a Gröbner basis for I.

If $v_i = f_i^<$ and v_i is not a multiple of v_j for $i \neq j$, in $Mag(X)$, then F is a Gröbner basis of I by Corollary 6.1.

Otherwise we choose a pair (i, j), $i \neq j$, such that v_i is a divisor of v_j.

Let f_j' be a normal form of f_j relative to $\{f_i\}$. Then the leading term of f_j' is smaller than v_j.

Let $F' := \{f_1', \ldots, f_n'\}$ with $f_i' := f_i$ for $i \neq j$.

Then $I(F) = I(F')$. We repeat the procedure just described for F now with F'. Thus we get a sequence $F^{(k)} = \{f_1^{(k)}, \ldots, f_n^{(k)}\}$, $n \geq 1$, with $(F^{(k)})' = F^{(k+1)}$ as long as $F^{(k)}$ does not satisfy the assumption of Corollary 6.1.

This sequence cannot be infinite. If it were to be infinite, there would exist an index i such that the leading term $v_i^{(k)}$ of $f_I^{(k)}$ would not be constant as a function of k. As it is decreasing, this is a contradiction to the well-ordering property of $<$.

Remark. The procedure just described can sometimes also be applied if F is infinite in cases where it is given by "regular" expressions.

It leads to theoretical results as in Section 9.

8. Hilbert series

Assume now that the set X of variables of $K\{X\}$ is equipped with a grading function $d : X \to \mathbb{N}_{\geq 1}$ of finite type which means that $\{x \in X : d(x) = r\}$ is finite for all $r \in \mathbb{N}$.

The generating series $G_X(t)$ of X is defined to be the power series

$$\sum_{r=0}^{\infty} \sharp\{x \in X : d(x) = r\} \cdot t^r \in \mathbb{C}[[t]].$$

There is a unique morphism $deg_d = deg : Mag'(X) \to \mathbb{N}$ such that $deg(1) = 0$, $deg(x) = d(x)$ for all $x \in X$. It is referred to as the degree induced by d.

Let V_r be the K-vector space generated by the monomials of degree r. Then $K\{X\} = \bigoplus_{r=0}^{\infty} V_r$ and this decomposition turns $K\{X\}$ into a graded algebra.

The Hilbert series $H_{K\{X\}^t}$ of this graded algebra is defined as

$$\sum_{r=0}^{\infty}(dim(V_r))t^r \in \mathbb{C}[[t]].$$

Now let $<$ be an admissible order on $Mag'(X)$ and J a homogeneous ideal in $K\{X\}$. This means that $J = \oplus^{\infty} =_{r=0} (J \cap V_r)$. Let Γ be the reduced Gröbner basis of J; it is a system of homogeneous polynomials.

If $I = J^< = \{f^< : f \in I,\ f \neq 0\}$, then I is a magma ideal in $Mag'(X)$.

If Ω is the minimal set of ideal generators of I, then the map $f \mapsto f^<$ is a correspondence between Γ and Ω. The degree function provides a grading of finite type on Γ and on Ω and the generating series $G_\Gamma(t)$ of Γ coincides with the generating series $G_\Omega(t)$ of Ω.

Proposition 8.1. *Let $A = K\{X\}/J$ be the graded algebra of classes modulo J and let $H_A(t)$ be the Hilbert series of A.*

Then

$$H_a(t) = 1 + q(G_X(t) - G_\Gamma(t))$$

where $q(t) = 1/2(1 - \sqrt{1-4t}) = \displaystyle\sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} t^{n+1}.$

Proof. (1) In the first step we prove the statement in the case $J = \{0\}$. Then $\Gamma = \emptyset$ and we have to show that

$$H_{K\{X\}}(t) = 1 + q(G_X(t)).$$

Now $H_{K\{X\}}(t) = 1 + G_M(t)$ for $M = Mag(X)$.

We have to show that

$$G_M(t) = q(G_X(t)).$$

Now let $G_X(t) = \displaystyle\sum_{r=1}^{\infty} \alpha_r \cdot t^r$, $G_M(t) = \displaystyle\sum_{r=1}^{\infty} \beta_r t^r$; then $\alpha_r = \sharp X_r$, $X_r = \{x \in X : d(x) = r\}$ and $\beta_r = \sharp M_r$, $M_r = \{m \in M : deg(m) = r\}$.

Then $\alpha_1 = \beta_1$ as $X_1 = M_1$.

Now let $r > 1$. Then M_r is the disjoint union

$$\bigcup_{i=1}^{r-1} M_i \cdot M_{r-i} \cup X_r.$$

As $\sharp M_i \cdot M_{r-i} = \beta_i \beta_{r-i}$, it follows that

$$\beta_r = \sum_{i=1}^{r-1} \beta_i \beta_{r-1} + \alpha_r.$$

Therefore $G_M(t) = G_M(t)^2 + G_X$ and as $q(G_X(t)) - q(G_X(t))^2 = G_X(t)$ it follows that $G_M(t) = q(G_X(t))$.

(2) Assume now that $J \neq \{0\}$. Then I is not empty. Let $G_I(t) = \sum_{r=1}^{\infty} \gamma_r t^n$. Then $\gamma_r = \sharp I_r$ where $I_r = \{v \in I : deg(v) = r\}$ and $\gamma_1 = \sharp \Omega_r$ where $\Omega : r = \omega \cap M_r$.

Now let $r \geq 2$. Then I_r is the disjoint union of Ω_r with the disjoint union of the sets

$$(I_{r-i} \cdot M_i \cup M_{r-i} \cdot I_i)$$

for $1 \le i \le r-1$. Also $I_{r-i} \cdot M_i \cong I_{r-i} \times M_i$ and $M_{r-i} \cdot I_i \cong M_{r-i} \times I_i$ as the multiplication map $M \times M \to M$ is injective. Also it is easy to check that $(I_{r-i} \cdot M_i) \cap (M_{r-i} \cdot I_i) = I_{r-i} \cdot I_i$; it follows that

$$\sharp(I_{r-i} \cdot M_i \cup M_{r-i} \cdot I : i) = \gamma_{r-i} \cdot \beta_i + \beta_{r-i}\gamma_i - \gamma_{r-i}\gamma_i$$

where $G_M(t) = \sum_{r=1}^{\infty} \beta_r t^r$.

Consequently

$$G_I(t) = 2G_I(t)G_M(t) - G_I(t)^2 + G_\Omega(t).$$

It follows that

$$G_I(t) = G_M(t) - 1/2 + 1/2\sqrt{1 - 4(G_X(t) - G_\Omega(t))}.$$

As $H_A(t) = H_{K\{X\}} - G_I(t)$ we get a proof of the formula. □

9. Generating series for non-graded algebras

Let A be any K-algebra with a unit and let X be a system of algebra generators for A. We choose a function $d : X \to \mathbb{N}_{\ge 1}$ of finite type and a total order on X.

There is a unique surjective K-algebra homomorphism $\eta : K\{X\} \to A$ induced by the embedding of X into A. Thus A is isomorphic with the algebra $K\{X\}/J$ of classes modulo the ideal J which is defined to be the kernel of η.

We choose an admissible order $<$ on $Mag(X)$ which extends the order on X.

Let N be the K-vector space of normal forms of J relative to $<$.

Then N is a graded linear subspace of $K\{X\}$, i.e. $N = \oplus_{r=0}^{\infty} N_r$ where N_r is generated by the elements of degree r in $Mag(X) - I$, where $I = \{f^< : f \in J,\ f \neq 0\}$.

We denote by $G_N(t)$ the generating series of N which is defined by

$$G_N(t) = \sum_{r=0}^{\infty} (dim(N_r))t^r.$$

This series depends on A, on X and on the admissible order $<$. It is also denoted by $G_{(A,X,<)}(t)$.

Proposition 9.1. *$G_{(A,X,<)}(t) = 1 + q(G_X(t) - G_\Gamma(t))$ where $G_\Gamma(t)$ is the generating series of the reduced Gröbner basis Γ of J.*

Proof. It is essentially the same as the proof of Proposition 8.1 above. □

Corollary 9.1. *$G_\Gamma(t) = G_X(t) + G^2(t) - 3G(t) + 2$ if $G(t) = G_{(A,X,<)}(t)$.*

Proof. $3G(t) - 2 - G^2(t) = (G(t) - 1) - (G(t) - 1)^2 = q(G_X(t) - G_\Gamma(t)) - q^2(G_X(t) - G_\Gamma(t)) = G_X(t) - G_\Gamma(t)$, as $q(t) - q^2(t) = t$. □

Example. Let A be the $\mathbb{R}$-algebra of Cayley numbers. It is generated by $X = \{i, j, k\}$. A complete system of relations is given in Shafarevich (1990), §19, D, p. 199.

We consider the elements of X to be of degree 1 and let $<$ be the degree first factor order on $Mag(X)$ for which $i < j < k$. Rajaee (in press) has computed the generating series $G(t) = G_{(A,X,<)}(t)$ to be $1 + 3t + 3t^2 + t^3$. Thus the generating series of the reduced Gröbner basis Γ of the ideal J of relations has the following generating series:

$$G_\Gamma(t) = 3t + G(t)^2 - 3G(t) + 2$$

as $q(t) - q(t)^2 = t$.
Thus

$$G_\Gamma(t) = 6t^2 + 17t^3 + 15t^4 + 6t^5 + t^6.$$

Saeed Rajaee has also computed the reduced Gröbner basis Γ for J. The element of degree 6 in it is $(i(jl))^2 - 1$.

10. Non-associative or tree power series

Let $K\{X\}$ denote the K-algebra of tree polynomials in a graded set X of variables of finite type. For any $f \in K\{X\}$, $f \neq 0$, let $ord(f)$ be the smallest element $r \in \mathbb{N}$ such that there is a monomial v in f of degree r whose coefficient in f is different from zero. Then $|f| := (1/2)^{ord(f)}$ is a valuation on $K\{X\}$ if $|0| := 0$. It defines a topology on $K\{X\}$.

The completion $K\{\{X\}\}$ of $K\{X\}$ with respect to this metric is the algebra of tree power series in X.

At this point I would like to cite a few results on special tree power series.

Let $\mathbb{Q}\{\{x\}\}$ denote the $\mathbb{Q}$-algebra of tree power series in one variable x over $\mathbb{Q}$. There is a unique derivation $\frac{\mathrm{d}}{\mathrm{d}x}$ on $K\{\{x\}\}$ such that $\frac{\mathrm{d}}{\mathrm{d}x}(x) = 1$. We denote $\frac{\mathrm{d}}{\mathrm{d}x}(f)$ also by $f'(x)$. The following results have been proved in Drensky and Gerritzen (2002).

There is a unique $E(x) \in \mathbb{Q}\{\{x\}\}$ such that

$$E'(0) = 1,$$
$$E(x) \cdot E(x) = E(2x).$$

Moreover $E'(x) = E(x)$, where $E'(x)$ denotes the derivative of $E(x)$ relative to x.

The tree power series $E(x)$ is called the non-associative exponential series and will be denoted by e^x or $\exp(x)$.

Also there is a unique $L(x) \in \mathbb{Q}\{\{x\}\}$ such that

$$L(0) = 0,$$
$$L'(0) = 1,$$
$$L(2x + x^2) = 2 \cdot L(x).$$

Moreover,

$$\exp(\log(1 + x)) = 1 + x,$$
$$\log(\exp(x)) = x.$$

The series $\log(1 + x) = L(x)$ is called the tree logarithm in x.

Formulas for the coefficients of the tree exponential $\exp(x)$ have been computed in Gerritzen (2003). There appears to be an interesting relation with Mersenne primes. It also occurs for the coefficients of

$$\cos(x) = 1/2(\mathrm{e}^{\mathrm{i}x} + \mathrm{e}^{-\mathrm{i}x}), \quad \sin(x) = \frac{1}{2\mathrm{i}}(\mathrm{e}^{\mathrm{i}x} - \mathrm{e}^{-\mathrm{i}x}), \quad \mathrm{i} = \sqrt{-1},$$

and of $\cos^2(x) + \sin^2(x)$ which is not equal to 1.

For any $v \in Mag'\{x\}$ let $a(v)$ be the coefficient of $\exp(x)$ with respect to v. We will describe a combinatorial formula for these coefficients.

For a natural number n, we denote by M_n the n-th Mersenne number $2^n - 1$. The Mersenne factorial $n!_M$ is defined to be the product $\prod_{i=1}^{n} M_i$ of all Mersenne number $M_1, \ldots, M_n$ while the Mersenne binomial $\binom{n}{r}_M$ is defined to be

$$\frac{n!_M}{r!_M (n-r)!_M}$$

for natural numbers r between 0 and n. One gets the recursive formula

$$\binom{n}{r}_M = \binom{n-1}{r}_M + 2^{n-r}\binom{n-1}{r-1}_M$$

from which one deduces that all $\binom{n}{r}_M$ are integers.

Note that Mersenne binomials are q-binomials for $q = 2$; see Kac and Cheung (2002), section 4.5, for the definition and properties of q-binomials.

Let

$$\omega(n) := \frac{2^{n-1} \cdot (n-1)!_M}{n!}$$

and $\tilde{a}(v) = n!\, \omega(n)\, a(v)$. Then $\tilde{a}(v) \in \mathbb{N}$ and

$$\tilde{a}(v) = \prod \binom{n(a) - 2}{n_1(a) - 1}_M$$

where the product is extended over all inner nodes a of the tree v and $n(a)$ is the degree of the tree t_a below a (in the direction to the leaves of v) and $n_1(a)$ is the degree of the left factor of t_a. This result is deduced in Gerritzen (2003).

In Gerritzen and Holtkamp (2003) the tree Hausdorff series $H(x, y) = \log(\mathrm{e}^x \mathrm{e}^y)$ in two variables over $\mathbb{Q}$ was studied. There is an analogue to the Baker–Campbell–Hausdorff formula.

Now there is emerging a theory of tree calculus, as it is obvious that there is an abundance of classical formulas for which there is a deformation into the non-associative setting. For example the concept of Taylor expansion has a useful extension to the non-associative setting; see Gerritzen and Holtkamp (2003).

A very important aspect is connected with compositions of power series.

Let $G = Aut(K\{\{x\}\}$ be the group of automorphisms of $K\{\{x\}\}$. Any $\varphi \in G$ is completely determined by the series $\varphi(x)$ whose order is 1. The inverse ψ of φ is given by a power series $\psi(x)$ such that $\varphi(\psi(x)) = 0$.

D. Zeilberger has asked whether there is an analogue of the classical inversion formula of Lagrange for computing the inverse series $\psi(x)$. At the moment there is no answer to this question.

I mention a result which will be proved elsewhere: G is essentially dual to the Hopf subalgebra of Connes and Kreimer of binary trees. It generalizes results of Connes and Muscovici who have considered a special case; see for instance Connes and Kreimer (2000) and Foissy (2002), section (6.2) and Proposition 194.

These considerations have to be generalized. Let $P(X)$ be the set of isomorphism classes of finite planar rooted trees which are not necessarily binary. For each $n \geq 2$, there is an n-ary grafting multiplication which associates with an n-tuple $(v_1, \ldots, v_n)$ of such trees a new tree by taking the disjoint union of $v_1, \ldots, v_n$, adding a new root r and edges between r and the roots r_i of v_i for all i.

Let K[[P(X)]] denote the algebra of power series of the algebraic system

$$(P(X), \cdot\, n, \geq 2).$$

D. Zeilberger has raised the question of extending the definition of exp, log to this setting. It seems that there has not been any research on this problem.

I expect the group of automorphisms of $K[[P(\{X\})]]$ to be essentially dual to the Hopf algebra of Connes and Kreimer. This comes out of the computation of the expansion substituting a power series into a planar rooted tree for which examples are given in Gerritzen and Holtkamp (2003), Section 6.

The concept of Gröbner bases for these power series algebras will certainly be of importance. I give a few details for the algebras $K\{\{X\}\}$.

Let $<$ be an admissible order on $Mag'(X)$ and $f \in K\{\{X\}\}$, $f \neq 0$.

Denote by $f_<$ the minimal element v in $Mag'(X)$ for which the coefficient of f relative to v is not zero. Then $deg(f_<) = ord(f)$.

If $f_< = 1$, then f is right and left invertible in $K\{\{X\}\}$ and an ideal in $K\{\{X\}\}$ containing f is equal to the unit ideal $K\{\{X\}\}$.

Let J be a closed ideal $\neq \{0\}$ in $K\{\{X\}\}$, $\Gamma \subseteq J$, $0 \notin \Gamma$.

Definition. Γ is called a Gröbner basis of J if $\Gamma_< := \{g_< : g \in \Gamma\}$ is a system of generators of the magma ideal $J_< := \{f_< : f \in J,\ f \neq 0\}$.

Proposition 10.1. *Let $\Gamma \subset K\{\{X\}\}$. Assume that $g_< \notin \langle h_< \rangle$ for all $g, h \in \Gamma$, $h \neq g$.*

Then Γ is a minimal Gröbner basis of I. This means that it is a Gröbner basis of I, but any proper subset of Γ is not a Gröbner basis of I.

Proof. It is essentially along the same lines as the proof of the Proposition 6.1. □

Definition. A Gröbner basis Γ of J is called reduced if:

(i) All leading coefficients of all $g \in \Gamma$ are 1 (i.e. the coefficient $c_m(g) = 1$ if $m = g_<$ and c_m denotes the coefficient relative to m).
(ii) If $g \in \Gamma$, $v \in Mag'(X)$ and the coefficient $c_v(g) \neq 0$, then $v \notin\ magma$, the ideal generated by the set $\Gamma_<$ of leading coefficients of elements of Γ.

Proposition 10.2. *Let J be an ideal in $K\{\{X\}\}$. Then J has a unique reduced Gröbner basis.*

Proof. For any $f \in K\{\{X\}\}$, $v \in Mag'(X)$, let $c_v(f)$ be the coefficient of f with respect to v.

Assume that Γ is a minimal Gröbner basis of J, $J \neq \{0\}$.

For any $g \in \Gamma$ let $V_g := \{v \in I := J_< : v \notin \Omega := \Gamma_<, c_v(g) \neq 0\}$. Let m be the smallest element in the union of all V_g.

Fix a $g \in \Gamma$ for which $m \in V_g$. Then m is a multiple in $Mag(X)$ of some $h_<$ with $h \in \Gamma$. Assume that $w_0, \ldots, w_r$ is a path between $h_<$ and m. This means that $w_0 = h_<$ and $w_i = w_{i-1} \cdot q_{i-1}$ or $q_{i-1} \cdot w_{i-1}$ for all $i > 1$ with $q_i \in Mag(X)$.

Let $\hat{w}_0 := h$ and $\hat{w}_i = \hat{w}_{i-1} \cdot q_{i-1}$ if $w_i = w_{i-1} \cdot q_{i-1}$, or $\hat{w}_i = q_{i-1} \cdot \hat{w}_{i-1}$ if $w_i = q_{i-1} \cdot w_{i-1}$. Then the smallest term of $\hat{w}_r$ is m and if $g' = g - \lambda \hat{w}_r$ for some suitable $\lambda \in K$ we get that $(g')_< = g_<$ and $c_m(g') = 0$. It also follows that $c_v(g') = 0$ for $v < m$, $v \neq g_<$.

Repeating this procedure we get for any $g \in \Gamma$ a converging sequence $g^{(k)}$ such that $(g^{(k)})_< = g_<$ and $c_v(g^{(k)}) = 0$ if $v \in I - \Omega$ with $deg(v) < k$. Let $\bar{g} := \lim_{k \to \infty} g^{(k)}$.

Then $\bar{\Gamma} := \{\bar{g} : g \in \Gamma\}$ is a reduced Gröbner basis of J if the smallest coefficient of any $g \in \Gamma$ is equal to 1.

The uniqueness statement is trivial. □

This concept can be used to classify the space of closed ideals in $K\{\{X\}\}$. In particular, one has the following result.

Corollary 10.1. *Let I be a magma ideal and assume that if $v, w \in Mag(X)$, $v < w$ and $v \in I$, then also $w \in I$.*

Then there is only one ideal J in $K\{\{X\}\}$ for which $J_< = I$.

It is the monomial ideal in $K\{\{X\}\}$ generated by I.

Proof. If Γ is the reduced Gröbner basis of J, then any $g \in \Gamma$ must be a monomial. □

11. Non-associative relations for the free associative algebra

Let $Mon(X)$ be the monoid freely generated by X. There is a canonical morphism $\eta : Mag(X) \to Mon(X)$ such that $\eta(x) = x$ for all $x \in X$. In Reutenauer (1993), (4.1), $\eta(w)$ is called the foliage of $w \in Mag(X)$. There is a unique morphism $deg : Mon(X) \to (\mathbb{N}, +)$ such that $deg(1) = 0$, $deg(x) = d(x)$ for all $x \in X$.

The associative K-algebra $K\langle X\rangle$ with a unit freely generated by X is the monoid algebra $K[Mon(X)]$ of $Mon(X)$ over K.

The morphism $\eta : Mag(X) \to Mon(X)$ extends to a K-algebra homomorphism $\bar{\eta} : K\{X\} \to K\langle X\rangle$. If $J_a = ker(\bar{\eta})$ then J_a is a ideal in $K\{X\}$ and $K\langle X\rangle \cong K\{X\}/J_a$.

Now let $<$ be the degree first factor ordering constructed in Section 3.

Let $w = x_1 x_2 \cdots x_n \in Mon(X)$ be a word of length $n \geq 1$, $x_i \in X$ for all i. Define $c(w) = x_1$ if $n = 1$ and $c(w) := x_1 \cdot c(x_2 \cdot \cdots \cdot x_n) \in Mag(X)$. It is easy to check that $c(w) \leq v$ for all $v \in Mag(X)$ with $\eta(v) = w$.

Let $r \geq 3$ and $\Gamma_r := \{c(v)c(w) - c(vw) : v$ is a word of length $n \geq 2$, $n < r$ and w is a word of length $r - n$ over $X\}$. One can show:

Proposition 11.1. *$\Gamma := \cup_{r=3}^{\infty} \Gamma_r$, is a Gröbner basis of J_a.*

Proof. (1) For any $v \in Mag(X)$ let $|v|$ be the underlying planar binary tree in $Mag(\{\zeta\})$ of v.

Then $g_v := v - c(\eta(v)) = 0$ if and only if $|v|$ is a right comb ζ^n defined by $\zeta^1 = \zeta$ and $\zeta^n := \zeta \cdot \zeta^{n-1}$ for $n > 1$. Also $c(\eta(u)) = |v|(u_1, \ldots, u_n)$ if $\eta(v) = u_1 u_2, \ldots o u_n \in Mon(X)$ with $u_i \in X$.

Then $g_v^< = v$ if $g_v \neq 0$.

It is easy to check that the system

$$\{g_v : v \in Mag(X), g_v \neq 0\}$$

is a K-basis of J_a.

Also $J_a^< = \{v \in Mag(X) : |v|$ is not a right comb$\}$. $J_a^<$ is a magma ideal in $Mag(X)$ because $|v_1 \cdot v_2| = |v_1| \cdot |v_2|$ and $|v_1 \cdot v_2|$ is a right comb only if $|v_1| = \zeta$ and $|v_2| = \zeta^{n-1}$ for some n.

(2) Let Ω be the minimal set of generators of $J_a^<$.

We show that $\Omega = \Gamma$.

Let $t \in J_a^<, t = t_1 \cdot t_2$. If $t \in \Omega$, then both $t_1, t_2 \notin J_a^<$ and $|t_1|, |t_2|$ are both right combs in $Mag(\{\zeta\})$. In this case $t_i = c(\eta(t_i))$ and $t \in \Gamma$.

If $t \in \Gamma$, then obviously $t = t_1 \cdot t_2$ with $t_1, t_2 \notin J_a^<$ and $|t_1|, |t_2|$ are right combs. If t is a proper multiple of some $v \in J_a^<$, then $|v|$ is a factor of $|t_1|$ or $|t_2|$ and is thus also a right comb.

This is a contradiction which shows that $t \in \Omega$. □

Remark. The generating series $G_\Gamma(t)$ has been computed in Gerritzen (2000), Section 4. If $G(t) = G_X(t)$, then $G_\Gamma(t) = \frac{G(t)}{(1-G(t))^2}$.

12. Open problem: Free alternative algebras

Let $I_{alt}(X) = I$ be the ideal in $K\{X\}$ generated by $S = S_1 \cup S_2$ where

$$S_1 = \{f^2g - f(fg) : f, g \in K\{X\}\}$$
$$S_2 = \{fg^2 - (fg)g : f, g \in K\{X\}\}.$$

The algebra $Alt(X) := K\{X\}/I_{alt}(X)$ is called the alternative algebra freely generated by X; see Kuzmin and Shestakov (1995), (1,1), p. 201.

Now $K\{X\}$ is considered as a graded algebra as in Section 8 where the grading is induced by a function $d : X \to \mathbb{N}_{\geq 1}$ of finite type.

Let

$$E_1 = \{u^2v - u(uv) : u, v \in Mag(X)\}$$
$$E_2 = \{uv^2 - (uv)v : u, v \in Mag(X)\}$$
$$E_1' = \{(u_1u_2)v + (u_2u_1)v - u_1(u_2v) - u_2(u_1v) : u_1, u_2, v \in Mag(X)\}$$
$$E_2' = \{u(v_1v_2) + u(v_2v_1) - (uv_1)v_2 - (uv_2)v_1 : u, v_1, v_2 \in Mag(X)\}.$$

Proposition 12.1. (i) *$I_{alt}(X)$ is generated by $E \cup E'$ where $E = E_1 \cup E_2$ and $E' = E_1' \cup E_2'$.*
(ii) *$I_{alt}(X)$ is a graded ideal in $K\{X\}$.*
(iii) *If char$K \neq 2$, then $I_{alt}(X)$ is generated by E'.*

Proof. (1) Let $f_1, f_2, g \in K\{X\},\ g = f_1 + f_2$. Then $h = f^2g - f(fg) \in I$ and $h = h_1 + h_2 + \hat{h}$ with $h_1 = f_i^2g - f_1(f_1g)$, $h_2 = f_2^2g - f_2(f_1g)$ and $\hat{h} = (f_1f_2)g + (f_2f_1)g - f_1(f_2g) - f_2(f_1g)$.

As $h, h_1, h_2\} \in I$, we also have $\hat{h} \in I$ for all $f_1, f_2, g \in K\{X\}$.

(2) In the same way one can see that $\tilde{h} := f(g_1g_2) + f(g_2g_1) - (fg_1) - (fg_1)g_2 - (fg_2)g_1 \in I$ for all $f, g_1, g_2 \in K\{X\}$.

(3) From (1), (2) we conclude that $E \cup E' \subseteq I_{alt}(X)$.

(4) Now let $f = \sum_{i=1}^{r} f_i, g = \sum_{k=1}^{s} g_k$. Then $f^2g - f(fg) = \sum_{\substack{1\leq i\leq j\leq r\\ 1\leq k\leq s}} \hat{h}_{ijk}$ with

$$\hat{h}_{iik} = f_i^2g_k - f_i(f_ig_k)$$
$$\hat{h}_{ijk} = (f_if_j + f_jf_i)g_k - f_i(f_jg_k) - f_j(f_ig_k) \qquad \text{if } i < j.$$

If now $f_i = \lambda_iu_i, \lambda_i \in K, u_i \in Mag'(X)$, and $g_k = \mu_kv_k, \mu_k \in K, v_k \in Mag'(X)$, then $\hat{h}_{ijk} = \lambda_i\lambda_j\mu_k[(u_iu_j + u_j + u_ju_i)v_k - u_i(u_jv_k) - u_j(u_iv_k)]$ for $i \leq j$ and thus $f^2g - f(fg)$ is contained in the ideal generated by $E \cup E'$.

(5) As in step (4) one proves that $fg^2 - (fg)g$ is contained in the ideal generated by $E \cup E'$.

(6) From (2) to (5) one can conclude that I_{alt} is generated by $E \cup E'$ because if $u = 1$ or $v = 1$, then $u^2v - u(uv) = 0$ and also $uv^2 - (uv)v = 0$.

(7) As $E \cup E'$ is a system of homogeneous polynomials for any choice of the grading function d, we see that $I_{alt}(X)$ is a graded ideal.
(8) If $u_1 = u_2$, then $2u^2v - 2u(uv) \in E'$ and thus $u^2v - u(uv)$ is contained in the ideal generated by E' if *char* $K \neq 2$. In the same way one sees that $uv^2 - (uv)v$ is contained in the ideal generated by E'. $\square$

A theorem of Artin—see Kuzmin and Shestakov (1995), (2.3), p. 224—states that $Alt(x)$, $Alt(\{x, y\})$ are associative, but $Alt(X)$ is not associative if $\sharp X \geq 3$.

We raise the question of determining the reduced Gröbner basis Γ for $I_{alt}(X)$ and its generating Hilbert series for any choice of a degree function d on X.

Acknowledgement

I would like to thank Teo Mora and Doron Zeilberger for helpful discussions and the referees for valuable hints.

References

Bourbaki, N., 1971. Algebra. Hermann, Paris (Chapters I–X).
Bergman, G., 1978. The Diamond lemma in ring theory. Adv. Math. 29, 178–218.
Buchberger, B., 1965 An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal. Ph.D. Thesis, University of Innsbruck, Institute for Mathematics (in German).
Brouder, Ch., Frabetti, A., 2003. QED Hopf algebras on planar binary trees. J. Algebra 267, 298–322.
Bokut, L.A., Kukin, G.P., 1994. Algorithmic and Combinatorial Algebra. Kluwer Academic Publishers, London.
Burris, S., Sankappanavar, H.P., 1981. A course in Universal Algebra. http://www.thoralf.uwaterloo.ca/htdocs/ualg.html.
Becker, T., Weispfennig, V., 1993. Gröbner Bases: A Computational Approach to Commutative Algebra. Springer-Verlag, New York.
Connes, A., Kreimer, D., 2000. Renormalization in quantum field theory and the Riemann–Hilbert problem I: The Hopf algebra structure of graphs and the main theorem. Comm. Math. Phys. 210, 249–273.
Cannon, J.J., Playoust, C., 1997. An Introduction to Algebraic Programming with Magma. University of Sydney.
Drensky, V., Gerritzen, L., 2002. Non-associative exponential and logarithm (Manuscript).
Foissy, L., 2002. Les algebres des Hopf des arbres enracines decores. These, Universite de Reims Champagne Ardenne.
Gerritzen, L., 1994. Grundbegriffe der Algebra. Vieweg.
Gerritzen, L., 2000. Hilbert Series and Non-associative Gröbner Bases. In: Manuscripta Math., vol. 103. Springer-Verlag, Heidelberg.
Gerritzen, L., 2003. Mersenne Binomials and the Coefficients of the Non-associative Exponential. Bochum (Manuscript).
Gerritzen, L., 2003. On the non-associative sine and cosine. Bochum (Manuscript).
Gerritzen, L., Holtkamp, R., 1998. On Gröbner bases of noncommutative power series. Indag. Math. N.S. 9 (4), 503–519.
Gerritzen, L., Holtkamp, R., 2003. Co-addition for free non-associative algebras and the Hausdorff series. J. Algebra 265, 264–284.
Ginzburg, V.A., Kapranov, M.M., 1994. Koszul duality for operads. Duke Math. J. 76.
de Graaf, W.A., Wisliceny, J., 1999. Constructing bases of finitely presented Lie algebras using Gröbner bases in free algebras. In: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation. Vancouver, BC. ACM, New York, pp. 37–43.
Harary, F., 1968. Graph Theory. Addison-Wesley, London.
Kurosh, A., 1947. Non-associative free algebra and free products of algebra. Res. Math. (Mat. Sbornik) N.S. 20 (62), 238–262.
Kac, V., Cheung, P., 2002. Quantum Calculus, Universitext. Springer.
Knuth, D.E., 1973. The Art of Computer Programming. In: Fundamental Algorithmus, vol. 1. Addison-Wesley, Reading.
Kuzmin, E.-N., Shestakov, I.P., 1995. Non-Associative Structures. In: Kostrikin, A.I., Shafarevich, (Eds.), Encyclopedia of Mathematical Sciences. In: Algebra VI, vol. 57. Springer-Verlag.
Lazard, M., 1955. Lois de groupes et analyseurs. Ann. Ecole Norm. Sup. Paris 72.
Li, H., 2002. Noncommutative Gröbner Bases and Filtered–Graded Transfer. In: Lecture Notes in Mathematics, vol. 1795. Springer-Verlag.

Loday, J.L., Ronco, M.O., 1998. Hopf algebra of the planar binary trees. Adv. Math. 139, 293–309.
Mora, T., 1994. An introduction to commutative and non-commutative Groebner bases. Theoret. Comput. Sci. 134, 131–173.
Madlener, K., Reinert, B., 1993. Computing Gröbner bases in monoid and groups rings. In: Proc. ISSAC'93. ACM, pp. 254–263.
Reutenauer, C., 1993. Free Lie Algebras. Oxford Univ. Press.
Rajaee, S., 2003. Bochum (Manuscript) (in press).
Shafarevich, I.R., 1990. Basic notions of algebra. In: Kostrikin, A.I., Shafarevich, (Eds.), Encyclopaedia of Mathematical Sciences. In: Algebra I, vol. 11. Springer-Verlag.
Ufnarovskij, V.A., 1995. Combinatorial and Asymptotic Methods in Algebra. In: Encyclopaedia of Mathematical Sciences, vol. 57. Springer-Verlag, Berlin.
Zacharias, G., 1978. Generalized Gröbner bases in commutative polynomial rings. Bachelor's Thesis, M.I.T.